［南投縣仁愛國小］（115）學年度第（一）學期辦理提升資訊素養活動執行成果表			
活動名稱	手機資訊安全的第一課		
辦理日期	115 年 9 月 15 日	出席人數	35 人
參加對象	■教職員工 ■學生 ■家長 □一般民眾		

宣導方式及內容：

手機資訊安全的第一課，核心在於建立「防護意識」與「基礎設定」，從日常使用習慣阻斷多數的資安風險。智慧型手機儲存了大量的個人隱私、金融帳戶與通訊紀錄，因此保護手機就是保護個人資產。以下為新手必學的五大基礎防護重點：

一、 帳號與螢幕鎖定防護

1.設定高強度鎖屏密碼。 避免使用生日、連續數字或簡單圖形作為解鎖密碼，並建議搭配指紋或臉部等生物辨識功能兼顧安全與便利。

2.開啟雙重驗證（2FA）。 為重要的社群、信箱與金融帳號綁定簡訊或驗證器 App，即使密碼外洩也能多一層保護。

3.各平台密碼不共用。 避免所有網路服務都使用同一組密碼，防止單一網站資料外洩時連帶波及其他帳號。

二、 應用程式（App）與系統管理

1.僅從官方商店下載軟體。 堅持透過 Google Play 或 Apple App Store 安裝程式，切勿點擊來路不明的網頁連結安裝 APK 或描述檔。

2.定期更新作業系統與 App。 系統更新通常包含最新的安全漏洞修補，發現有更新通知時應盡快安裝。

3.嚴格審查 App 權限。 安裝與使用軟體時，留意其要求的權限是否合理，例如手電筒 App 不應要求存取聯絡人或位置資訊。

三、 網路連線與傳輸安全

1.謹慎使用免費公共 Wi-Fi。 在咖啡廳、機場等場所連上無密碼的 Wi-Fi 時，避免進行網路銀行轉帳或輸入信用卡資料。

2.關閉閒置的無線功能。 在公共場合未使用藍牙、NFC 或個人熱點時建議暫時關閉，降低被惡意裝置掃描或強制連線的風險。

四、 識別釣魚與社交工程陷阱

1.不點擊可疑簡訊與連結。 收到自稱銀行、物流或政府機關的異常通知簡訊時，務必先透過官方客服查證，切勿直接點擊附帶的短網址。

2.防範實體窺視。 在大眾運輸工具或人多處輸入密碼時，留意周遭是否有旁人偷看螢幕（肩窺）或監視器角度。

五、 資料備份與遺失應變

1.養成定期備份習慣。 利用雲端硬碟或電腦定期備份重要照片與聯絡人，萬一手機中毒或損壞時能快速復原資料。

2. **開啟「尋找我的裝置」功能。** 事先啟用系統內建的遠端定位與清除資料功能，若不幸遺失手機時可立即鎖定並抹除敏感資訊。

照片（請貼１～２張照片）：





請將成果存成 PDF 格式再上傳（可利用 office2007 以上，另存 pdf 格式，或其他方式轉存 PDF。）